COVER SHEET

Justice Environments Conference
Ensuring the Integrity of the E-court Process
Ros Macdonald, Mark Burdon, Sheryl Jackson*

Abstract

This paper considers possible implications of information protection within Australia's e-court processes. While judgements on the directed use of courtroom technologies during proceedings and current practice directions provide some indication of the thoughts that underlie the use of IT in court proceedings, a literature review conducted by the research team has revealed that there is a distinct lack of formal research and more work is required to fully address the issue of information protection and e-courts.

Introduction

Since 2000 technology has begun to play a more important role in the operation of courts around Australia. After a hesitant start, Australia's court services are moving towards acceptance of information technology as an integral component of many court processes. Initial development was reactive and *ad hoc* in nature in that new courtroom technologies were implemented to meet the technology demands of several very complex pieces of criminal and civil litigation and by lengthy commissions of inquiry in the early 1990s[1].

Increasing efficiency and effectiveness are very much the focus for these new technologies. They were first used to automate and catalogue massive volumes of information and evidence into manageable forms using electronic case management databases[2]. Once data was in an electronically searchable format, the focus changed from automation to presentation of evidence through document imaging systems. This in turn stimulated a growth in animated presentations of complex and key evidence. Real time transcription enabled lawyers and judges to record notes and to immediately recall what was said during previous days of evidence. Courts also began to use video conferencing facilities for vulnerable witnesses[3]. Digital recording was used to capture visual evidence, such as Aboriginal dance rituals in native title claims[4], which could be played back and viewed at the court's discretion.

While the development of court technologies has expanded, initial research into e-courts has revealed that there has been little attention directed to information

* Ros Macdonald is a senior lecturer in the School of Law Queensland University of Technology, Mark Burdon is a lawyer and a senior research assistant in the Institute of Information Security and Sheryl Jackson is the acting Head of the School of Law QUT.
[1] R Macdonald and A Wallace, 'Review of the extent of courtroom technology in Australia' (2004) 12(3) *William and Mary Bill of Rights Journal* 649 'The Challenge of the Information Society: Application of Advanced Technologies in Civil Litigation and Other Procedures: Report on Australia' (Paper presented at the XI World Congress on Procedural Law, Vienna, 23-28 August 1999)
[2] R Macdonald and A Wallace, 'Review of the extent of courtroom technology in Australia' (2004) 12(3) *William and Mary Bill of Rights Journal* 649
[3] 'The Challenge of the Information Society: Application of Advanced Technologies in Civil Litigation and Other Procedures: Report on Australia' (Paper presented at the XI World Congress on Procedural Law, Vienna, 23-28 August 1999)
[4] *De Rose v State of South Australia* [2002] FCA 1342

protection issues that play an integral part in other industries. An example of this point is the case law and practice directions which dictate the use of courtroom technology in trials.

Current practice in e-courts

Definitions

Before going any further, an attempt is warranted at defining an electronic court. What is it?
It may be a courtroom that has nothing more in it than some computers, linked to each other if possible, but at least linked to the Internet. Opposing counsel and the judge would have computers and the court manager or associate would have access to a system that allows electronic documents to be displayed to the jury and witnesses on monitors or large screens. This system would also be linked to an electronic database that contains all the information that, in its primary form, is electronic information, suitably indexed, so it can easily be retrieved for viewing. There needs to be a mechanism for making exhibits from this evidence, for review of evidence, and for searching across the database. At the present time, these facilities are available in proprietary software, of which the three marketed and most widely available in Australia are *Ringtail CaseBook/CourtBook, Systematics Benchmark* series, and *Summation iblaze*.

These programs, which are accessible across the Internet using passwords, are protected at the application stage but are designed for Microsoft Windows and that is not a secure system. Indeed, such "malware" as "keyboard sniffers" and allied virus, rootkit and other similar programs may compromise entities such as passwords entered into a computer keyboard, capture relevant files and forward them to third parties, etc. In these cases, the problems in security lie with the basic, underlying computer operating systems and data network interfaces rather than with the actual computer application itself.

Perhaps the best definition of an electronic court comes from a recent Australian court case - *Harris Scarfe v Ernst & Young* [2005] SASC 407 -

> 'The electronic court enables the trial to be conducted to a large extent in a "paperless" fashion. It goes beyond the electronic storage and retrieval of relevant documents on the court file, such as pleadings, particulars, lists of documents and notices to admit. It includes electronic presentation of witness statements, expert reports, chronologies, lists of authorities and outlines of argument. More significantly the database includes documents which will be, or are likely to be, tendered and the electronic version of the transcript. There is the option of incorporating real time transcript of the proceedings. …
>
> 'Relevant documents, and if necessary more than one document at a time, are able to be displayed to persons in the courtroom on computer screens set up for this purpose. In the courtroom itself counsel, solicitors, the witness, the judge and the judge's associate each have such facilities available. Users have the ability to "freeze" a document they wish to keep in front of them, make annotations to documents and transcript, which annotations will be accessible only by that user, and to move between related documents and transcript by way of hyperlinks. The system allows for the orderly

> marking of documents for identification and the marking of exhibits, including references to the basis of tender, any qualifications on tender and admission, and transcript references at the point of tender together with subsequent referrals by witnesses and counsel to that exhibit' [at para 18].

As you can see, such a court is quite technologically advanced. A subsidiary question here is whether it allows for efficient and effective disposal of cases. There are few judicial pronouncements on this point, and these do not rely on empirical evidence in support. In the case from which the passage above has been taken, the judge had to decide when in the litigation process the actual scanning of documents had to begin. The plaintiff and the first defendant were happy for the entire case to be 'run' electronically; the second and third defendants were worried about cost and utility of the technology, and indeed, whether the court could order the electronic court to be used. In the end, after looking at perceived advantages of electronic courts, the judge directed that the electronic court should be used, concluding that the power was available to so direct. The point to note is that there was no empirical evidence on which he could base its assessment of improved efficiency apart from statements from other courts and his own belief, from personal experience.

Technology, in the sense of electronic court practice, has not been enthusiastically embraced by the legal profession, particularly in Queensland. True, this statement depends on what is meant by 'technology', as virtually every legal practitioner uses a personal computer and email on a regular and consistent basis. Technology here means the scanning of documents into databases or the keeping of electronic documents in databases, so that instead of paper based traditional trials there is the potential for reduced reliance on paper with a corresponding developing use of electronic courtbooks

Judicial pronouncements on information security

One of the factors mentioned by Bleby J in the *Harris Scarfe* case, and others, leading the court to take a favourable view of electronic courts, is security.
Justice Bleby himself says –

> 'The electronic court enables the parties, the trial judge and court staff to have secure access to all of the material in an efficient manner both in and out of the courtroom.' [para 18]

In the leading case on the use of electronic courts, *Idaport Pty Ltd v National Australia Bank (No 6)* [2000] NSWSC 338, Einstein J said, in directing use of an electronic court –

> '59 Then there is the fact that the Technology Court is said to be secure. It has been specifically described, as I have understood it, as "its own island", in terms of court room access on this parameter. It has an internal network within the court room. …
>
> 60 There is judicial access to a research facilities network, the internet and also limited telephone capacity. Many situations apparently involve case software, which as Ms Taggart has indicated, have a web interface which allows

> secure access over the web by external sources into the case management systems in offices. From the bar table, one is able, through the web, to access such case management systems (where such systems are in place), into solicitors' offices and possibly Counsels' chambers. That facility, I have been informed, is available through the use of the Technology Court. Ms Taggart is able to provide the parties with a direct internet connection through telephone lines from the bar table itself. One would then search discovery documents and other documents through that mode.
>
> 61 I have mentioned secure access for the bar table and the bench. That access I have referred to, in terms of internet access, dial out or access via external case systems which the bar table might require. Each person with access, if that was an option taken up, would have a secure telephone "dial in" through the Attorney General's fire wall into the server which would be set up for the case.'

In the only other case dealing with electronic courts, *Kennedy Taylor (Vic) Pty Ltd v Grocon Pty Ltd* [2002] VSC 32, security is not raised.

In both the cases referred to where security is mentioned, it is taken at face value that the advice about security from proprietary and commercial level software suppliers is correct. There was no examination of the work of technical information security experts on the issue. In the 'rush' to provide what is seen as 'a just, quick and cheap resolution of the real issues in civil proceedings' (the overriding purpose) [*Supreme Court Rules 1970 (NSW)* r 3(1)(2)] there has been no independent consideration of overall information system security. A point to note is that if each court was indeed 'its own island', issues of information protection would not so readily arise. However, once connection is made to the Internet and other external organisations the unknown level of security implementation creates a risk to the integrity and confidentiality (if necessary) of information. Those administering the electronic court lose control once access progresses through to a third party or external system. The security implemented and the administration of that security on the external system or systems is then relied upon.[5]

Practice Directions

Guidelines on the use of courtroom technologies do exist in the form of practice directions. However, these directions do not have an information protection outlook. For example, the Supreme Court of New South Wales published Practice Note No 105 *Use of Technology in Civil Litigation* in March 1999. That set the scene for the use of technology as an everyday tool in civil litigation in New South Wales. The New South Wales Note was used to some extent as a starting point for other jurisdictions although there are significant variations across jurisdictions. The note was replaced by Practice Note No 127 *Use of Technology in Civil Litigation*, with effect from 1 March 2004.

In South Australia, Practice Direction No 52 *Guidelines for the use of technology in litigation in any civil matter* was issued on 17 August 2001. The note was based on the generic draft practice note issued by the Australian Institute of Judicial

[5] Personal communication Dr Caroline Allinson, defence consultant, Canberra

Administration in 1999.[6] This practice direction applies to civil litigation in all South Australian courts.[7] The South Australian Practice Direction generally reflects the consensus approach adopted by the higher courts, with a purpose of providing for and encouraging the use of information technology, to the extent appropriate, in civil litigation in all South Australian courts.

Finally, Queensland followed the lead of the other states, with the issue by the Supreme Court of Queensland on 13 July 2004 of Practice Direction No 8 of 2004: Electronic Management of Documents. It has been appropriately said of the Queensland Practice Direction that: "to fit the industry it is serving, the practice note is more conservative in its language and intent, but it nevertheless represents a sound first step for the Court".[8]

Courts and Information Protection

Courts have placed great importance on security, but not in the actual trial of matters. The focus has been on the mechanics of electronic lodgement of court documents using the Internet. For example, the Federal Court website tells us that in its e-court filing website the technology is–

> 'based on the Australian banking and electronic commerce industry standard Secure Socket Layer (SSL) security technology. SSL is cryptography technology that uses special codes - 128 bit keys - that encrypt messages sent over the Internet. SSL encryption turns a message into an unintelligible string of characters and symbols and makes it virtually impossible to decipher. In addition, if a message is somehow tampered with, SSL technology will detect the tampering and reject the message.'

The website goes on to say –

> 'Visitors who file documents on-line enter their credit card details into an electronic form with (sic) [which] is encrypted by SSL technology and is securely transmitted via the Court's e-filing service provider (Creative Digital Technology) to its merchant facility provider (the ANZ Bank). The Court or its technology service provider does not store customer credit card details at any time during this process. Visitors who use this facility are provided the same level of security as if they were using an automatic teller machine (ATM) or performing an EFTPOS transaction.'

There are, however, continuing concerns about the levels of information security for Internet transactions. In his 2003 address to the *Courts for the 21st Century: Public access, privacy, security* Conference at the QUT School of Law, Professor Bill Caelli addressed some potential pitfalls by highlighting inherent technological protection issues in a recently published e-court proposal in the *Sydney Morning Herald*. The presentation focused on several fundamental information protection mechanisms and widely accepted design misconceptions including connectivity, end-to-end secure channels, archiving, time/date stamping and electronic signatures. Even so, court

[6] http://www.aija.org.au/info/techn/guideciv.htm
[7] The Practice Direction stands as Supreme Court Practice Direction 52, District Court Practice Direction No 10, and Magistrates Court Practice Direction No 1 of 2001.
[8] Sandra Potter, "Tech Support – Effective use of IT in civil litigation" *Lawyers Weekly*, 9 May 2003 14 at 15.

managers have not paid any special attention to technology in the court itself, relying, it seems, on the proprietary software providers to provide the security. The Federal Court of Australia did run a complete electronic trial in very adverse conditions in outback South Australia [*de Rose v Fuller and State of South Australia* [2002] FCA 1342]. The stated aim was to

> 'examine issues of standards and protocols for courtroom technology; and identify best practice'.

A report on the conduct of the case [http://www.federalcourt.gov.au/ecourt/ecourt_strategy.html visited 7.01.2006] concluded that -

> 'The experience in de Rose suggests that data consistency, the integrity of the data and structural predictability are essential.'

Further, the report identified issues that would be important in any future electronic trials. At the top of the list are identification of consistent standards and security. The Court has given notice that it will issue guidelines and practice notes to parties and practitioners about the circumstances when an electronic trial might be considered, which guidelines etc would include technical information. They have not appeared so far.[9]

What needs to be addressed as security issues in e-courts?[10]

What may or may not be evident from this paper so far is that there has not been a single defining moment at which e-court technology was embraced. Circumstances have been such, over a protracted period of time, that particular technology has been sourced because a particular need has arisen. In Australia the use of technology has been driven by large complex litigation cases, where enormous numbers of documents have had to be retrieved, catalogued and sorted. In the first Australian case of note in which electronic databases were used, the *Estate Mortgages* case, one of the lawyers involved claimed that;

> '[u]nless we took over the Tennis Centre [where the Australian Open is played each summer], there's no practical way we could have conducted the case without the system' [*Technology and the Law* Victorian Law Reform Commission, 1999 ch 10]

It was estimated in that case that there were upwards of 800,000 documents retrieved and catalogued, with 1.7 million pages of information in them. Because of this *ad hoc*

[9] The Federal Court and the Victorian, New South Wales and Queensland Supreme courts all have Practice notes/statements/directions that give guidance on protocols for electronic document discovery and in some cases, appeal books. However, as the Federal Court practice note was written in 2000, I assume that what the report is means here are additional matters, not covered in the Practice Note of April 2000.

[10] For this part of my paper I am indebted to Dr Lauren May and Mr Mark Burdon, who have addressed these issues in a draft of a paper '*Ensuring the Integrity of the e-court Process'* they are preparing for a Research Network for a Secure Australia (RNSA) conference in Wollongong in May 2006.

approach to electronic information management, there have never been any uniform sets of standards produced. Various jurisdiction around Australia have drafted practice directions for electronic document disclosure/discovery, in which suggestions have been made for how to number documents, how to objectively and subjectively code document fields, when to employ electronic document discovery methods, when to consider electronic trials etc. None of these practice directions, statements, notes and guidelines discuss any aspects of security.

The overriding security issue for e-courts lies in the integrity of the court process. As May and Burdon write

> 'The court system requires certainty to function but new technologies, implemented without a rigorous information protection perspective, could lead to a new technological structure which has an insubstantial foundation of virtual holes.'

They suggest that the areas of focus should lie in the development of trusted information security systems in concert with the increasing sophistication of technological processes themselves. They continue –

> 'Our preliminary findings indicate that court systems are planning to expand the use of court technology and to re-align existing processes around new information technologies. Consequently, the scope of the potential problem will increase commensurate with the implementation of these new technological structures and processes that have not been conclusively tested within a information security context.'

The solution ?

There are no overriding uniform standards across the Australian jurisdictions that allow for –

> 'the creation of an information protection framework, including policies and standards that can be used by courts to *define the use of court technologies* and to ensure that their implementation is grounded within firm information security principles.' [May and Burdon]

E-courts and Information Protection– An Area of Study

Current case law and practice directions are predominantly based on facilitating the efficient and effective use of courtroom technologies within proceedings. They do not cover the information protection issues in depth and they are not intended to set standards for parties to adhere to. Courts have been concerned with information protection but from an e-filing perspective. Accordingly, little or no attention has been given to information protection issues during trial and other court proceedings.

A QUT research team, comprised of academics from the Law and IT Faculties has started a research project that will look at this very issue – information protection implications of the newly developing e-courts. So far in this research a literature review has been conducted that supports the team's thesis that little work has been carried out.

QUT Research on E-Courts

QUT has developed a unique body of expertise in the areas of e-courts and information protection.

The Law Faculty's <e.law> Moot Court is one of Australia's most advanced electronic courtroom containing state-of-the-art information technology and audio-visual integration. It uses the latest software and hardware and is constantly being upgraded in line with latest developments. School of Law academics undertake research into various aspects of electronic court practice and disseminate research via the Law Faculty's annual e-court seminar and conference programme. The programme is run in conjunction with the Supreme Court of Queensland and conference themes have included e-courts: access, security and privacy; managing technology in litigation and access for the disadvantaged.

To conduct this research, the Law School has begun working with QUT's Information Security Institute (ISI), which is a multi-disciplinary institute that builds practical solutions for government, business and the community by undertaking research in technology, legal, policy and governance issues related to information security.

The Literature Review

The purpose of the literature review was defined as follows:

> *To explore the areas of e-Courts, e-Litigation and IT use in the legal profession, with emphasis on Information Security (IS) issues, to provide an impetus, definition and framework for future ISI research in these areas.*

The researchers deliberately took a broad approach to the literature review because the area of interest is still in development, and it was difficult to quantify whether an initial literature search would retrieve a large or small number of references. As it transpired, the search produced a large volume of relevant materials.

The Research Areas

Four principal areas were covered in the literature search as all four encompassed the use of court technologies in some form or another. The areas are:

1. E-courts;
2. E-litigation;
3. IT use in the legal profession; and
4. Information protection use in 1-3.

The definition of an e-court for the purpose of the review was a court that makes use of information technology to run its proceedings. The technologies used include: document imaging, real-time transcription, case management databases, video control, external web access and email access to law firms. The new technologies are predominantly used to enhance parties' presentations to the court, case management and to save court time.

E-courts are the driving force for e-litigation. Three substantive subsets of e-litigation exist: e-filing, e-disclosure and e-discovery. E-filing is the formal submission of documentation to courts using electronic means. E-disclosure is the process of litigants exchanging electronic documents and objectively tagged metadata in a prearranged format E-discovery is similar to the process of computer forensics as it involves finding information usually after the fact; for example, emails.

Given the drive for e-courts and e-litigation, the researchers believed that it was important for the initial research to gain some understanding of the use of information technology in law firms and the legal profession. Like the court system, the law profession is a standard bearer for information protection principles given the nature of confidential and personally sensitive information in use. The researchers therefore wished to ascertain what technologies were being used and whether systems were designed around information security principles.

Information protection for the research is concerned with ensuring a quality of service for e-courts, e-litigation and law firms. Typically it is concerned with confidentiality, integrity and availability of information. Specific requirements are determined by individual applications.

Initial Literature Review Findings

In total, 1,795 references were retrieved. The number of references for each area is as follows:

Area	**Number of References**	**% of Total Number**
E-courts	566	31.5
E-Litigation	463	25.8
Information Technology in the legal profession	483	26.9
Information Protection	283	15.8
Total	1795	100

It is immediately apparent that there are significantly fewer references on the area of information protection than the other three areas (15.8%). Information protection has not figured highly in much academic discussion about court systems and for the legal profession. By far the most common type of reference retrieved are journal articles. The top twenty journals provide a useful snapshot of the topic's overall importance. The majority of journals are designed for the American market and they tend to be professional rather than academic (i.e. New Jersey Law Report, Colorado Lawyer, etc.).

Name of Journal	**Number of References**
National Law Journal	62
American Bar Association Journal	58

Name of Journal	Number of References
Trial	48
Law Institute Journal	46
New York Law Journal	37
Computers and Law UK	36
Lawyers Weekly	27
Computer Law & Security Report	22
New Jersey Law Journal	22
Colorado Lawyer	21
E.Law Practice	21
Judges' Journal	21
Federal Lawyer	20
Law Society Journal	20
California Lawyer	18
John Marshall Journal of Computer & Information Law	18
Illinois Bar Journal	16
Journal of Information, Law and Technology	16
Legal Assistant Today	15
Solicitors Journal	15
Texas Bar Journal	15

Most references are from the law and technology and professional legal journals. The former are predominantly peer reviewed where as the latter are not. References featured in pure law and pure technology journals are very small in number. Accordingly, most quality references appear in the cross disciplinary law, information and technology journals, which are published in most jurisdictions. Most of this type journal originates in the United States, followed by the United Kingdom.

Further, the majority of references are largely descriptive, in that they describe what technologies are currently in use in the spheres of e-courts, e-litigation and law firms. By and large, published articles are not peer reviewed. Approximately 20% of the references have been peer reviewed and the vast majority of those are largely conceptual in their analysis.

The Need for Formal Research

The evidence so far shows that there is a distinct lack of empirical research, in the areas of e-courts. Many of the claims by published authors have not been supported by empirical results. For example, many authors suggest that the use of technology in e-courts and e-litigation makes both processes more cost effective and efficient. Yet there is virtually no empirical evidence to support these assertions.

Not surprisingly, there is no methodological basis to the body of literature that has developed. This includes both quantitative and qualitative research designs. Existing research methodologies have focused on the area of IT use in the legal profession and

they could provide a template for future research. However, there is nothing similar in the area of e-courts. It is perhaps a little disconcerting that a body of literature containing nearly 1,800 references has developed without any formal, academic research methods or focus.

Practically no research in this area has been conducted on e-courts.

The literature review so far supports the researchers' contention that new technologies in the court system may not have been founded on information protection principles. There are few materials examining information protection concepts or practices involving the adoption of new court technologies.

Conclusion

This research is still in its infancy but enough has been done o form some initial views. The researchers' believe that there is a lack of serious research in the body of literature on e-courts and information protection. Much of the attention has been on the court technologies themselves and perhaps too little has been paid to their potential impacts and consequences.

There are plenty who say that these new technologies deliver a more efficient and effective system yet there is no empirical research to support that assumption. Finally, there is very little work about the potential damage that could be caused to the integrity of the court process by implementing technologies that are not founded on sound information protection principles.

The aim of research that is being undertaken by our small group within the Information Security Institute (ISI) at QUT is to develop a generic information protection framework incorporating a set of standards that can be applied across the entire e-litigation and e-court area to achieve a level of security that meets the standard of other industries. Indeed, there could be questions about whether appropriate security standards need to be met by the computer systems and data networks employed in court situations. In this regard, due deference must be given to existing and emerging national and international standards in the information security area, for example, International Standard 15408, the "common criteria" for the security assessment/evaluation of information technology products and systems. Electronic court practice, the technology, the court process, including legislation and rules, and the cost will all be scrutinized.

The ultimate aim is to come up with a safe, secure and generic set of standards (and even possibly a "*court operating system*") that is a model of best practice based on developed universal standards These do not exist at present. Along the way it is hoped to make some recommendations about 'best-practice' court practice for electronic courts and to find out, through research, comparative costs of electronic as against traditional litigation practice.

Is information security is necessary in the e-court process? Over the course of the past year, a senior court administrator and a prominent academic in the area have been asked the same question. The view of the court administrator is that it is not an issue because the documents are on the public record anyway, and the academic's view is

that the security issues are best left to the proprietary software suppliers! I suggest that if we do that we are closing the door after the horse has bolted especially as this all assumes that those documents incorporated into the court electronic records are themselves the correct and authentic documents and that their integrity, in storage, is guaranteed !